ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 111 (2005) 190–196

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

On the range of a covering function

Zhi-Wei Sun[1]

Department of Mathematics and Institute of Mathematical Science, Nanjing University, Nanjing 210093, People's Republic of China

Received 6 April 2004; revised 21 September 2004

Communicated by D. Goss

Available online 1 Februraury 2005

Abstract

Let $\{a_s(\mathrm{mod}\, n_s)\}_{s=1}^k$ $(k>1)$ be a finite system of residue classes with the moduli $n_1, \ldots, n_k$ distinct. By means of algebraic integers we show that the range of the covering function $w(x) = |\{1 \leqslant s \leqslant k : x \equiv a_s \,(\mathrm{mod}\, n_s)\}|$ is not contained in any residue class with modulus greater one. In particular, the values of $w(x)$ cannot have the same parity.

MSC: primary 11B25; secondary 11A07; 11A25; 11B75; 11R04.

Keywords: Cover of $\mathbb{Z}$; Covering function; Erdős–Selfridge conjecture

1. Introduction

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, let $a(n)$ stand for the residue class $\{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$. A finite system

$$\{a_s(n_s)\}_{s=1}^k \quad (k > 1) \tag{1.1}$$

of residue classes is said to be a *cover* of $\mathbb{Z}$ if $\bigcup_{s=1}^k a_s(n_s) = \mathbb{Z}$.

E-mail address: zwsun@nju.edu.cn.

URL: http://pweb.nju.edu.cn/zwsun.

[2] Supported by the National Science Fund for Distinguished Young Scholars (No. 10425103) and the Key Program of NSF (No. 10331020) in P. R. China.

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2004.11.004

The concept of cover of $\mathbb{Z}$ was introduced by Erdős [E50] in the early 1930s, who was particularly interested in those covers (1.1) with the moduli $n_1, \ldots, n_k$ distinct. By Example 3 of the author [S96], if $n > 1$ is odd then

$$\{1(2), 2(2^2), \ldots, 2^{n-2}(2^{n-1}), 2^{n-1}(n), 2^{n-1}2(2n), \ldots, 2^{n-1}n(2^{n-1}n)\}$$

forms a cover of $\mathbb{Z}$ with distinct moduli. Covers of $\mathbb{Z}$ have been studied by various researchers (cf. [G04,PS]) and many surprising applications have been found (see, e.g. [F02,S00,S01,S03b]).

Here are two major open problems concerning covers of $\mathbb{Z}$ (see sections E23, F13 and F14 of [G04] for references to these and other conjectures).

Erdős–Selfridge Conjecture. *Let (1.1) be a cover of $\mathbb{Z}$ with distinct moduli. Then $n_1, \ldots, n_k$ cannot be all odd and greater than one.*

Schinzel's Conjecture. *If (1.1) is a cover of $\mathbb{Z}$, then there is a modulus n_t dividing another modulus n_s.*

For system (1.1), the function $w : \mathbb{Z} \to \mathbb{Z}$ given by

$$w(x) = |\{1 \leqslant s \leqslant k : \ x \in a_s(n_s)\}| \tag{1.2}$$

is called its *covering function*. Obviously $w(x)$ is periodic modulo the least common multiple $N = [n_1, \ldots, n_k]$ of the moduli $n_1, \ldots, n_k$.

Now we list some known results concerning the covering function $w(x)$.

(i) The arithmetic mean of $w(x)$ with x in a period equals $\sum_{s=1}^{k} 1/n_s$.

(ii) (Sun [S95,S96]) The covering function $w(x)$ takes its minimum on every set of

$$\left|\left\{0 \leqslant \theta < 1 : \sum_{s \in I} \frac{m_s}{n_s} - \theta \in \mathbb{Z} \text{ for some } I \subseteq \{1, \ldots, k\}\right\}\right|$$

consecutive integers, where $m_1, \ldots, m_k$ are given integers relatively prime to $n_1, \ldots, n_k$, respectively.

(iii) (Sun [S03a]) The maximal value of $w(x)$ can be written in the form $\sum_{s=1}^{k} m_s/n_s$ with $m_1, \ldots, m_k \in \mathbb{Z}^+$.

(iv) (Porubský [P75]) If $n_1, \ldots, n_k$ are distinct, then $[n_1, \ldots, n_k]$ is the smallest positive period of the function $w(x)$.

(v) (Sun [S03a]) If $n_0 \in \mathbb{Z}^+$ is a period of the function $w(x)$, then for any $t = 1, \ldots, k$ we have

$$\left\{\sum_{s \in I} \frac{1}{n_s} : I \subseteq \{1, \ldots, k\} \setminus \{t\}\right\} \supseteq \left\{\frac{r}{n_t} : r \in \mathbb{Z} \text{ and } 0 \leqslant r < \frac{n_t}{(n_0, n_t)}\right\},$$

where (n_0, n_t) denotes the greatest common divisor of n_0 and n_t.

(vi) (Sun [S04]) The function $w(x)$ is constant if $w(x)$ equals a constant for $|S|$ consecutive integers x where

$$S = \left\{ \frac{r}{n_s} : \ r = 0, \ldots, n_s - 1; \ \ s = 1, \ldots, k \right\}.$$

In this paper we study the range of a covering function (via algebraic integers) for the first time. Proofs of the theorems below will be given in the next section.

Theorem 1.1. *Suppose that the range of the covering function of* (1.1) *is contained in a residue class with modulus* m. *Then, for any* $t = 1, \ldots, k$ *with* $mn_t \nmid [n_1, \ldots, n_k]$, *we have* $n_t \mid n_s$ *for some* $1 \leqslant s \leqslant k$ *with* $s \neq t$.

Corollary 1.1. *If the covering function* $w(x)$ *of* (1.1) *is constant, then for any* $t = 1, \ldots, k$ *there is an* $s \neq t$ *such that* $n_t \mid n_s$, *and in particular* $n_k = n_{k-1}$ *provided that* $n_1 \leqslant \cdots \leqslant n_{k-1} \leqslant n_k$.

Proof. Suppose that $w(x) = c$ for all $x \in \mathbb{Z}$. Choose an integer $m > [n_1, \ldots, n_k]$. As $c(m)$ contains the range of $w(x)$, the desired result follows from Theorem 1.1. $\square$

Remark 1.1. When (1.1) is a disjoint cover of $\mathbb{Z}$, i.e., $w(x) = 1$ for all $x \in \mathbb{Z}$, the first part of Corollary 1.1 was given by Novák and Znám [NZ] and the second part was originally obtained by Davenport, Mirsky, Newman and Radó independently. Corollary 1.1 appeared in Porubský [P75].

Corollary 1.2. *Suppose that those moduli in* (1.1) *which are maximal with respect to divisibility are distinct. Then* $w(\mathbb{Z}) = \{w(x) : x \in \mathbb{Z}\}$ *cannot be contained in a residue class other than* $0(1) = \mathbb{Z}$, *i.e., for any prime* p *there is an* $x \in \mathbb{Z}$ *with* $w(x) \not\equiv w(0) \pmod p$. *In particular, those* $w(x)$ *with* $x \in \mathbb{Z}$ *cannot have the same parity.*

Proof. Assume that $w(\mathbb{Z})$ is contained in a residue class with modulus $m \in \mathbb{Z}^+$. For each modulus n_t maximal with respect to divisibility, there is no $s \neq t$ such that $n_t \mid n_s$, thus mn_t divides $N = [n_1, \ldots, n_k]$ by Theorem 1.1. Since N is also the least common multiple of those moduli n_t maximal with respect to divisibility, we must have $mN \mid N$ and hence $m = 1$. This ends the proof. $\square$

Remark 1.2. In contrast with the Erdős–Selfridge conjecture, Corollary 1.2 indicates that *if* (1.1) *is a cover of* $\mathbb{Z}$ *with distinct moduli then not every integer is covered by* (1.1) *odd times.*

Here is another related result.

Theorem 1.2. *Let* $A = \{a_s(n_s)\}_{s=1}^k$ *and* $B = \{b_t(m_t)\}_{t=1}^l$ *both have distinct moduli. Then* A *and* B *are identical provided that* $w_A(x) \equiv w_B(x) \pmod m$ *for all* $x \in \mathbb{Z}$, *where w_A and w_B are covering functions of A and B, respectively, and m is an integer not dividing* $N = [n_1, \ldots, n_k, m_1, \ldots, m_l]$.

Remark 1.3. In 1975, Znám [Z75] extended a uniqueness theorem of Stein [St] as follows: Under the condition of Theorem 1.2, we have $A = B$ if $w_A = w_B$. This follows from Theorem 1.2 by taking $m > N$.

Theorem 1.1 can be refined as follows.

Theorem 1.3. *Let $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}$ be weights assigned to the k residue classes in (1.1), respectively. Suppose that $n_0 \in \mathbb{Z}^+$ is the smallest positive period of $w(x) = \sum_{1 \leqslant s \leqslant k,\, n_s \mid x - a_s} \lambda_s$ modulo $m \in \mathbb{Z}$, and that $d \in \mathbb{Z}^+$ does not divide n_0 but $I(d) = \{1 \leqslant s \leqslant k : d \mid n_s\} \neq \emptyset$. Then, either m divides $[n_1, \ldots, n_k] \sum_{s \in I(d)} \lambda_s / n_s$, or we have*

$$|I(d)| \geqslant |\{a_s \bmod d : s \in I(d)\}| \geqslant \min_{\substack{0 \leqslant s \leqslant k \\ s \notin I(d)}} \frac{d}{(d, n_s)} \geqslant p(d), \tag{1.3}$$

where $p(d)$ denotes the smallest prime divisor of d.

Remark 1.4. Theorem 1.3 in the case $m = 0$ was first obtained by the author [S91] in 1991, an extension of this was given in [S04].

Instead of (1.1) we can also consider a finite system of residue classes in $\mathbb{Z}^n$ (cf. [S04]) and deduce n-dimensional versions of Theorems 1.1–1.3.

2. Proofs of Theorems 1.1–1.3

Proof of Theorem 1.1. Without any loss of generality we assume that $0 \leqslant a_s < n_s$ for $s = 1, \ldots, k$. Set $N = [n_1, \ldots, n_k]$. Then

$$\begin{aligned}
\sum_{r=0}^{N-1} w(r) z^r &= \sum_{r=0}^{N-1} \sum_{\substack{1 \leqslant s \leqslant k \\ n_s \mid a_s - r}} z^r = \sum_{s=1}^{k} \sum_{\substack{0 \leqslant r < N \\ r \in a_s(n_s)}} z^r \\
&= \sum_{s=1}^{k} z^{a_s} \sum_{0 \leqslant q < N/n_s} (z^{n_s})^q \\
&= \sum_{\substack{1 \leqslant s \leqslant k \\ z^{n_s} = 1}} \frac{N}{n_s} z^{a_s} + (1 - z^N) \sum_{\substack{1 \leqslant s \leqslant k \\ z^{n_s} \neq 1}} \frac{z^{a_s}}{1 - z^{n_s}}.
\end{aligned}$$

Suppose that $w(r) = a + mq_r$ for each $r \in \mathbb{Z}$ where $a, q_r \in \mathbb{Z}$. If $\alpha \notin \mathbb{Z}$ but $\alpha N \in \mathbb{Z}$, then

$$\sum_{r=0}^{N-1} w(r)e^{2\pi i\alpha r} = m\sum_{r=0}^{N-1} q_r e^{2\pi i\alpha r}$$

and also

$$\sum_{r=0}^{N-1} w(r)e^{2\pi i\alpha r} = \sum_{\substack{s=1\\ \alpha n_s\in\mathbb{Z}}}^{k} \frac{N}{n_s} e^{2\pi i\alpha a_s},$$

therefore we have the following congruence:

$$\sum_{\substack{s=1\\ \alpha n_s\in\mathbb{Z}}}^{k} \frac{N}{n_s} e^{2\pi i\alpha a_s} \equiv 0 \pmod{m} \tag{2.1}$$

in the ring of all algebraic integers.

If $1 \leqslant t \leqslant k$ and $n_t \mid n_s$ for no $s \in \{1, \ldots, k\} \setminus \{t\}$, then by applying (2.1) with $\alpha = 1/n_t < 1$ we obtain that

$$\frac{N}{n_t} e^{2\pi i a_t/n_t} \equiv 0 \pmod{m}$$

and hence m divides N/n_t in $\mathbb{Z}$.

The proof of Theorem 1.1 is now complete. $\square$

Proof of Theorem 1.2. Without any loss of generality, we assume that $n_1 > \cdots > n_k$ and $m_1 > \cdots > m_l$. As $w_A(x) - w_B(x) \equiv 0 \pmod{m}$ for all $x \in \mathbb{Z}$, by modifying the proof of Theorem 1.1 slightly, we find that if $\alpha \notin \mathbb{Z}$ but $\alpha N \in \mathbb{Z}$ then

$$\sum_{\substack{s=1\\ \alpha n_s\in\mathbb{Z}}}^{k} \frac{N}{n_s} e^{2\pi i\alpha a_s} - \sum_{\substack{t=1\\ \alpha m_t\in\mathbb{Z}}}^{l} \frac{N}{m_t} e^{2\pi i\alpha b_t} \equiv 0 \pmod{m}. \tag{2.2}$$

In the case $d = \max\{m_1, n_1\} > 1$, by applying (2.2) with $\alpha = 1/d$ and the hypothesis $m \nmid N$, we get that $m_1 = n_1$ and

$$\frac{N}{d}(e^{2\pi i a_1/d} - e^{2\pi i b_1/d}) \equiv 0 \pmod{m}.$$

If $a_1 \not\equiv b_1 \pmod{d}$, then $z = 1 - e^{2\pi i(b_1-a_1)/d}$ is a zero of the monic polynomial $(-1)^{d-1}P(1-x) \in \mathbb{Z}[x]$ where $P(x) = (1-x^d)/(1-x) = 1 + x + \cdots + x^{d-1}$, hence z divides the constant term $P(1) = d$ of $P(1-x)$ in the ring of algebraic integers. As m does not divide N, we must have $a_1 \equiv b_1 \pmod{d}$ and so $a_1(n_1) = b_1(m_1)$. Now that

$$|\{1 < s \leqslant k : x \in a_s(n_s)\}| \equiv |\{1 < t \leqslant l : x \in b_t(m_t)\}| \pmod{m} \text{ for all } x \in \mathbb{Z},$$

we can continue the above procedure to obtain that

$$a_2(n_2) = b_2(m_2), \ \ldots, \ a_{\min\{k,l\}}(n_{\min\{k,l\}}) = b_{\min\{k,l\}}(m_{\min\{k,l\}}).$$

If $k \neq l$, say $k > l$, then $m\mathbb{Z}$ contains the range of the covering function of $\{a_s(n_s)\}_{s=l+1}^{k}$ and this contradicts Theorem 1.1 since $m \nmid [n_{l+1}, \ldots, n_k]$ and $n_{l+1} > \cdots > n_k$. So $A = B$ and we are done. $\square$

Proof of Theorem 1.3. Let $N = [n_1, \ldots, n_k]$. Clearly $(n_0, N) \in n_0\mathbb{Z} + N\mathbb{Z}$ is also a period of $w(x)$ mod m, so $(n_0, N) = n_0$ and hence $n_0 \mid N$. Observe that

$$\sum_{\substack{s=1 \\ x \in a_s(n_s)}}^{k} \lambda_s - \sum_{\substack{r=0 \\ x \in r(n_0)}}^{n_0-1} w(r) \equiv 0 \pmod{m}$$

for each $x \in \mathbb{Z}$. As in the proof of Theorem 1.1, if $c \in \mathbb{Z}$ and $d \nmid c$ then

$$\sum_{\substack{s=1 \\ (c/d)n_s \in \mathbb{Z}}}^{k} \lambda_s \frac{N}{n_s} e^{2\pi i \frac{c}{d} a_s} - \sum_{\substack{r=0 \\ (c/d)n_0 \in \mathbb{Z}}}^{n_0-1} w(r) \frac{N}{n_0} e^{2\pi i \frac{c}{d} r} \equiv 0 \pmod{m}. \tag{2.3}$$

For any $c \in \mathbb{Z}^+$ divisible by none of those $d/(d, n_s)$ with $0 \leqslant s \leqslant k$ and $s \notin I(d)$, we have

$$d \mid cn_s \iff \frac{d}{(d, n_s)} \mid c \iff d \mid n_s \iff s \in I(d),$$

therefore (2.3) yields that

$$\sum_{s \in I(d)} \lambda_s \frac{N}{n_s} e^{2\pi i \frac{c}{d} a_s} \equiv 0 \pmod{m}.$$

Let

$$R = \{0 \leqslant r < d : a_s \equiv r \pmod{d} \text{ for some s} \in I(d)\}$$

and suppose that $|R| < \min_{0\leqslant s\leqslant k,\, s\notin I(d)} d/(d, n_s)$. By the above,

$$u_n := \sum_{r\in R} c_r (e^{2\pi i \frac{r}{d}})^n \equiv 0 \pmod m \text{ for every } n = 1, \ldots, |R|,$$

where $c_r = N \sum_{s\in I(d),\, a_s\in r(d)} \lambda_s/n_s \in \mathbb{Z}$. As $\{u_n\}_{n\geqslant 0}$ is a linear recurrence of order $|R|$ with characteristic polynomial $\prod_{r\in R}(x - e^{2\pi i r/d})$ whose coefficients are algebraic integers, we have $u_n \equiv 0 \pmod m$ for every $n = |R|+1, |R|+2, \ldots$. In particular, $\sum_{r\in R} c_r = u_d \equiv 0 \pmod m$, i.e., m divides $N\sum_{s\in I(d)} \lambda_s/n_s$. We are done. $\square$

Acknowledgement

The author thanks the referee for his constructive comments.

References

[E50] P. Erdős, On integers of the form $2^k + p$ and some related problems, Summa Brasil. Math. 2 (1950) 113–123.

[F02] M. Filaseta, Coverings of the integers associated with an irreducibility theorem of A. Schinzel, Number Theory for the Millennium (Urbana, IL, 2000), vol. II, A.K. Peters, Natick, MA, 2002, pp. 1–24.

[G04] R.K. Guy, Unsolved Problems in Number Theory, 3rd ed., Springer, New York, 2004.

[P75] Š. Porubský, Covering systems and generating functions, Acta Arith. 26 (1975) 223–231.

[PS] Š. Porubský, J. Schönheim, Covering systems of Paul Erdős: past, present and future, in: G. Halász, L. Lovász, M. Simonvits, V.T. Sós (Eds.), Paul Erdős and his Mathematics. I, Bolyai Soc. Math. Studies, vol. 11, Budapest, 2002, pp. 581–627.

[NZ] B. Novák, Š. Znám, Disjoint covering systems, Amer. Math. Monthly 81 (1974) 42–45.

[St] S.K. Stein, Unions of arithmetic sequences, Math. Ann. 134 (1958) 289–294.

[S91] Z.W. Sun, An improvement to the Znám–Newman result, Chinese Quart. J. Math. 6 (3) (1991) 90–96.

[S95] Z.W. Sun, Covering the integers by arithmetic sequences, Acta Arith. 72 (1995) 109–129.

[S96] Z.W. Sun, Covering the integers by arithmetic sequences II, Trans. Amer. Math. Soc. 348 (1996) 4279–4320.

[S00] Z.W. Sun, On integers not of the form $\pm p^a \pm q^b$, Proc. Amer. Math. Soc. 128 (2000) 997–1002.

[S01] Z.W. Sun, Algebraic approaches to periodic arithmetical maps, J. Algebra 240 (2001) 723–743.

[S03a] Z.W. Sun, On the function $w(x) = |\{1\leqslant s\leqslant k : x \equiv a_s \pmod{n_s}\}|$, Combinatorica 23 (2003) 681–691.

[S03b] Z.W. Sun, Unification of zero-sum problems, subset sums and covers of $\mathbb{Z}$, Electron. Res. Announc. Amer. Math. Soc. 9 (2003) 51–60.

[S04] Z.W. Sun, Arithmetic properties of periodic maps, Math. Res. Lett. 11 (2004) 187–196.

[Z75] Š. Znám, On properties of systems of arithmetic sequences, Acta Arith. 26 (1975) 279–283.